PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-232775

(43)Date of publication of application : 27.08.1999

---

(51)Int.Cl. G11B 20/10

---

(21)Application number : 10-031846 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 13.02.1998 (72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

---

(54) CONTROL STANDARD MAKING METHOD, CONTROL STANDARD MAKING SYSTEM, AND MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable detecting an illegal terminal device before damage occurs more surely than conventional one.

SOLUTION: When data is required from a VTR device 1030 and the like having respective intrinsic EU 164 to STB 120, a certification means 211 performs certification based on the prescribed control standard about their data request, it is decided whether required data is transferred from STB 120 to the VTR device 1030 performing request or not in accordance with the certification result, and a data request history information storing means 212 sends data request history information including EU 164 of the VTR

device to a control device 110 in accordance with the certification result. The control device discriminates whether the VTR device 1030 is a regular one or not by the prescribed discrimination standard utilizing the data request history information, makes CRL based on the certification result, and sends it to the SBT 120.

LEGAL STATUS [Date of request for examination] 26.02.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3569123
[Date of registration] 25.06.2004
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] When there is a data demand to a data transfer unit from each data demand terminal unit which has the identifier of a proper, respectively, it is related with those data demands. As opposed to the data demand terminal unit which performed authentication based on predetermined authentication criteria, and performed said data demand from said data transfer unit according to the result of said authentication Or according to the result of said authentication, management equipment is received from said data transfer unit. a ******** [transmitting the demanded data] -- determining -- always -- The data demand hysteresis information containing said identifier of the data demand terminal unit delivery and said management equipment The management-criteria creation approach characterized by judging whether the data demand terminal unit contained in the data demand hysteresis information is regular, being based on the judgment result, and creating or updating management criteria by the predetermined criterion using said data demand hysteresis information sent.

[Claim 2] The group formed by two or more of said data demand terminal units and said data transfer units those with two or more groups, and said data demand hysteresis information The time information which specifies time of day with said data demand from said data demand terminal unit which has the identifier other than said identifier, Are information including the location information which specifies the location of the data demand terminal unit, and said predetermined criterion in said management equipment In all the data demand hysteresis information transmitted from said two or more data transfer units The management-criteria creation approach according to claim 1 characterized by being what determines the data demand terminal unit which compares said time information corresponding to an identifier and said location information on these plurality, respectively, and has an identifier with unjust possibility when two or more same identifiers exist.

[Claim 3] The management-criteria creation approach according to claim 2 characterized by creating or updating the unjust list of data demand terminal units considered that all the data demand terminal units that have these same identifiers were inaccurate things, and it was considered as said management criteria that were these inaccurate things when the data demand terminal unit which has an identifier with the judgment result by said criterion and said unjust possibility is determined.

[Claim 4] It is the management-criteria creation approach according to claim 3 which said management equipment transmits said all or some of unjust list to said data transfer unit, and is characterized by said data transfer unit performing said authentication, using said transmitted unjust list at least.

[Claim 5] The data transfer unit connected to each data demand terminal unit which has the identifier of a proper, respectively an unit or the management equipment to manage [two or more] The new registration information containing the identifier of the schedule which is sent and which is connected newly or said data demand terminal unit connected newly is used. By the predetermined criterion The management-criteria creation approach characterized by judging whether the data demand terminal unit corresponding to said new registration information is regular, being based on the judgment result, and creating or updating management criteria.

[Claim 6] The group formed by two or more of said data demand terminal units and said data transfer units those with two or more groups, and said data transfer unit When connection with said data transfer unit of said data demand terminal unit connected newly is detected, It is what transmits the new registration information on the data demand equipment to said management equipment. Said predetermined criterion The same identifier as the identifier contained in the new registration information whenever said new registration information is transmitted The management-criteria creation approach according to claim 5 characterized by being the criteria which judge whether it has already existed in the list of said identifiers currently transmitted and held from said two or more data transfer units.

[Claim 7] The management-criteria creation approach according to claim 6 characterized by creating or updating the unjust information on the data demand terminal unit considered that all the data demand terminal units that have these same identifiers were inaccurate things, and it was considered as said management criteria that were these inaccurate things when the judgment result by said criterion shows that said same identifier exists during said list.

[Claim 8] When it is shown that said same identifier exists during said list, it is considered that all the data demand terminal units that have these same identifiers are inaccurate things. the judgment result by said criterion -- (1) -- as said management criteria The unjust information on the data demand terminal unit it was considered that were these inaccurate things is created. When it is shown that said same identifier does not exist during said list, it is considered that the data demand terminal unit which has said identifier contained in said new registration information is a regular thing. or -- updating -- (2) -- as said management criteria [moreover,] The management-criteria creation approach according to claim 6 characterized by creating or updating the normal information on the data demand terminal unit it was considered that was the regular thing.

[Claim 9] Or said normal information is transmitted to said data transfer unit. said management equipment -- said all or a part of unjust information -- said data transfer unit When there is a data demand from each data demand terminal unit, it is related with those data demands. As opposed to the data demand terminal unit which attested using said transmitted unjust information or normal information at least, and performed said data demand according to the authentication result The management-criteria creation approach according to claim 8 characterized by being what determines whether transmit the demanded data.

[Claim 10] The management-criteria creation approach according to claim 4 or 9 which extracts the information corresponding to the data transfer unit and the data demand terminal unit which has a connection relation, and is characterized by transmitting among the information about the data demand terminal unit currently mentioned to said unjust information when said management equipment transmits said a part of unjust information to said data transfer unit.

[Claim 11] When there is a data demand from two or more data demand terminal units which have the identifier of a proper, respectively, and these data demand terminal unit, it is related with those data demands. As opposed to the data demand terminal unit which performed said data demand according to the result of the authentication the authentication based on predetermined authentication criteria -- carrying out -- (1) -- a ******** [transmitting the demanded data] -- determining -- (2) -- always -- or according to the result of the authentication with the data transfer unit which outputs the data demand hysteresis information containing said identifier of the data demand terminal unit [moreover,] Said said outputted data demand hysteresis information is acquired. By the predetermined criterion The management-criteria creation system characterized by having management equipment which judges whether the data demand terminal unit contained in the data demand hysteresis information is regular, is based on the judgment result, and creates or updates management criteria.

[Claim 12] The medium characterized by recording the program for making a computer perform any of claims 1-10, or all or a part of steps of each steps of one publication.

[Claim 13] The medium characterized by recording the program for making a computer perform the function of all or a part of means of each means according to claim 11.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the management-criteria creation approach, a management-criteria creation system, and a medium.

[0002]

[Description of the Prior Art] The receiver of dedication receiving, and recording on videotape the TV program sent by satellite broadcasting service with the VTR equipment connected to the receiver, or viewing and listening to it on television conventionally, is performed.

[0003] in this case, conditional [that by which record is forbidden in the image and voice data broadcast and conditional / record of is enabled only once] -- there are data. Therefore, in order to keep these conditions, it will be the requisite that recognize this condition correctly and a user side uses the equipment which operates to normal.

[0004] Then, when transmitting data recordable once from the receiver of dedication, for example to VTR equipment, usually authentication actuation for checking first whether the VTR equipment is the above regular equipments is performed. Data are not transmitted when it judges with it being inaccurate equipment which performs actuation which disregarded the above-mentioned conditions as a result of this authentication actuation.

[0005] Hereafter, it explains focusing on the conventional the configuration and authentication actuation of an exclusive receiver and a terminal unit, referring to drawing 12 .

[0006] Drawing 12 is the block diagram showing the conventional connection situation and conventional configuration of an exclusive receiver and a terminal unit.

[0007] As shown in this drawing, an antenna 1010 is a means to receive the broadcasting electric-wave from a satellite, and the satellite broadcasting service receiver (this is only hereafter called STB) 1020 is a means to change the broadcasting electric-wave which received into AV data. The data transmission line 1070 is a bus line for the data transmission in which STB1020 and each terminal unit described below were formed in between. moreover -- a terminal unit -- ****** -- VTR -- equipment -- (-- A --) -- 1030 -- VTR -- equipment -- (-- B --) -- 1040 -- a recording apparatus -- (-- C --) -- 1050 -- TV equipment (D) is further connected with STB1020 by the data transmission line 1070.

[0008] Next, the internal configuration of STB1020 is described further, referring to this drawing.

[0009] That is, the receiving means 1021 is a means to link directly with an antenna 1010, to restore to the received data, to cancel the scramble for broadcast given to the received data, and to separate the received data multiplexed further. The encryption means 1022 is a means to encipher AV data outputted from the receiving means 1021 by the work-piece key Kw for the encryption which it had beforehand with a compression condition. Moreover, the encryption means 1022 enciphers the work-piece key Kw using the subkey obtained from the authentication means 1023, and are the enciphered work-piece key and a means for outputting the both sides of AV data which carried out [above-mentioned] encryption to a terminal unit through the data I/O means 1024. In addition, it is because it is premised on it carrying out record etc. that it is necessary to also send the work-piece key enciphered as mentioned above to a terminal unit here after decrypting transmitted AV data in a terminal unit. The authentication means 1023 is a means to perform authentication using a predetermined secrecy function and to generate the subkey corresponding to an authentication partner as the result in order to confirm mutually whether each other's both equipments are equipment of normal between the terminal units which have carried out AV data transfer demand. Moreover, the authentication means 1023 makes all the secrecy functions (Sa, Sb, Sc, Sd, ..., Sn, ...) of the proper which all terminal units have correspond with those identification numbers, and is held. The data transfer force means 1024 is IEEE1394 known as a digital interface. The data transfer means 1024 is a means to perform two transfers, the isochronous transfer suitable for a data transfer like the image for which the guarantee of real time nature is needed, or voice, and the asynchronous transfer suitable for a transfer of a data for authentication, a command, etc. without the need.

[0010] Next, the internal configuration of VTR equipment (A) 1030 is described further.

[0011] The data transfer means 1031 is the same means as the data transfer means 1024, and is a means to receive the enciphered work-piece key and enciphered AV data as shown in this drawing. The authentication means 1032 is a means to have the secrecy function Sa of a proper beforehand, to generate the subkey Ksa as a result of authentication, and to output to the decryption means 1033. The decryption means 1033 is a means to decrypt the enciphered work-piece key which was obtained from the data transfer means 1031 by the subkey Ksa, and to decrypt AV data which restored the work-piece key Kw and were enciphered by the work-piece key Kw. Record / playback means 1034 is a means to record decrypted AV data and to reproduce the record data.

[0012] in addition -- others -- a terminal unit -- it is -- VTR -- equipment -- (-- B --) -- 1040 -- a recording device -- (-- D --) -- 1050 -- TV -- equipment -- (-- D --) -- 1060 -- record / playback means -- removing -- the configuration and basic target of the above-mentioned VTR equipment (A) 1030 -- being the same . However, the secrecy functions which each authentication means has beforehand will be Sb, Sc, and Sd, if it says in order of each above-mentioned equipment. Therefore, the subkeys generated by authentication with each equipment and STB1020 will be Ksb, Ksc, and Ksd, if it says in above sequence.

[0013] The content of authentication is described [in / next / the above configuration] briefly.

[0014] For example, when performing AV data transfer demand from VTR equipment (A) 1030 to STB1020, in advance of the activation, the following authentications are needed.

[0015] That is, first, the authentication means 1032 of VTR equipment (A) 1030 generates random numbers A1 and A2, and enciphers this with the secrecy function Sa. Here, the enciphered random number is indicated to be Sa (A1, A2). The authentication means 1032 transmits Sa (A1, A2) and the self identification number IDa to STB1020 through the data transfer means 1031 (step 1001). Here, the identification number is beforehand given by the number of each terminal unit proper.

[0016] In STB1020, through the data transfer means 1024, the authentication means 1023 obtains Sa (A1, A2) and an identification number IDa, recognizes the identification number, and chooses the secrecy function Sa corresponding to it from two or more held secrecy functions (step 1002). Thereby, the secrecy function which STB1020 should use for authentication between VTR equipment (A) 1030 is specified.

[0017] Next, Sa (A1, A2) in which the authentication means 1023 of STB1020 carried out [above-mentioned] reception using the secrecy function Sa is decoded, and the latter random number A2 is sent to VTR equipment (A) 1030 among A1 and A2 which were restored, without enciphering (step 1003).

[0018] Next, the authentication means 1032 of VTR equipment (A) 1030 compares A2 sent from STB1020 with the random number A2 which oneself generated at the above-mentioned step 1001. If both sides are in agreement, it can be judged that STB1020 is equipment of normal (step 1004).

[0019] Next, the authentication means 1023 by the side of STB1020 generates a random number B1 and B-2, and enciphers this with the secrecy function Sa. And Sa (B1, B-2) is transmitted to VTR equipment (A) 1030 (step 1005).

[0020] With VTR equipment (A) 1030, Sa (B1, B-2) in which the authentication means 1032 carried out [above-mentioned] reception using the secrecy function Sa is decoded, and latter random-number B-2 is sent to STB1020 among B1 and B-2s which were restored, without enciphering (step 1006).

[0021] Next, the authentication means 1023 compares B-2 sent from VTR equipment (A) 1030 with random-number B-2 which oneself generated at the above-mentioned step 1005. If both sides are in agreement, it can be judged that VTR equipment (A) 1030 is equipment of normal (step 1007).

[0022] By the above, that both both sides are equipment of normal can check mutually, it comes, authentication is completed, and AV data transfer to VTR equipment (A) 1030 is permitted.

[0023] Four random numbers A1, A2, and B1 and B-2 exist in the authentication means 1023 and 1032 of both equipments as a result of this authentication. Then, next, both authentication means 1023 and 1032 use random numbers A1 and B1, and generate the above-mentioned subkey Ksa, respectively. In addition, since not using a random number A2 and B-2 has the circumstances where these were transmitted without enciphering, on the occasion of generation of a subkey, those who use the random numbers A1 and B1 without such circumstances are because it sees from the safety of a key and excels more.

[0024] In the encryption means 1022, using the subkey Ksa generated by carrying out in this way, the work-piece key Kw is enciphered and AV data are enciphered by the work-piece key Kw. And the both sides of the AV data Kw (AV) enciphered as the work-piece key Ksa (Kw) by which encryption was carried out [above-mentioned] are outputted to VTR equipment (A) 1030 through the data I/O means 1024.

[0025] With VTR equipment (A) 1030, the decryption means 1033 decodes the encryption work-piece key Ksa (Kw) using the subkey Ksa obtained from the authentication means 1032, and decodes the encryption AV data Kw (AV) using the decoded work-piece key Kw.

[0026]

[Problem(s) to be Solved by the Invention] However, by the above authentication approaches, the inaccurate person copied the secrecy function Sn and the identification number IDn of regular equipment as it was just as it is, and when the inaccurate equipment which can perform the same authentication approach as the above was manufactured and sold and the inaccurate equipment was used, by the above-mentioned authentication approach, the equipment has not detected that it is inaccurate equipment, and was not able to prevent AV data transfer.

[0027] Generally, in the unauthorized use by the 3rd person, such as a theft ATM card, direct damage occurs notably to the owner of the ATM card. Therefore, it is possible to prevent an unauthorized use promptly. On the other hand, as accepting-station equipment of broadcast data, even if the above inaccurate equipments exist, there are particulars that damage to authorized personnel cannot surface easily. For example, even if it copies the data of the prohibition on a copy unjustly, and it is rare that the concrete damage in which royalties etc. are arrears surfaces and it surfaces, time amount most by it will have passed and it will also be expected that damage becomes serious.

[0028] Thus, by the conventional authentication approach, since a deer response was not able to be performed after damage comes to light, it had the technical problem that it was imperfect as the authentication approach.

[0029] This invention aims at offering the management-criteria creation approach that detection of inaccurate equipment can be ensured compared with the former, a management-criteria creation system, and a medium, in consideration of the technical problem of such a conventional approach.

[0030]

[Means for Solving the Problem] When this invention according to claim 1 has a data demand to a data transfer unit from each data demand terminal unit which has the identifier of a proper, respectively, it relates to those data demands. As opposed to the data demand terminal unit which performed authentication based on predetermined authentication criteria, and performed said data demand from said data transfer unit according to the result of said authentication Or according to the result of said authentication, management equipment is received from said data transfer unit. a ******** [transmitting the demanded data] -- determining -- always -- The data demand hysteresis information containing said identifier of the data demand terminal unit delivery and said management equipment It is the management-criteria creation approach which judges whether the data demand terminal unit contained in the data demand hysteresis information is regular, is based on the judgment result, and creates or updates management criteria by the predetermined criterion using said data demand hysteresis information sent.

[0031] This invention according to claim 5 the data transfer unit connected to each data demand terminal unit which has the identifier of a proper, respectively an unit or the management equipment to manage [two or more] The new registration information containing the identifier of the schedule which is sent and which is connected newly or said data demand terminal unit connected newly is used. By the predetermined criterion It is the management-criteria creation approach which judges whether the data demand terminal unit corresponding to said new registration information is regular, is based on the judgment result, and creates or updates management criteria.

[0032] Two or more data demand terminal units with which this invention according to claim 11 has the identifier of a proper, respectively, When there is a data demand from these data demand terminal unit, it is related with those data demands. As opposed to the data demand terminal unit which performed said data demand according to the result of the authentication the authentication based on predetermined authentication criteria -- carrying out -- (1) -- a ******** [transmitting the demanded data] -- determining -- (2) -- always -- or according to the result of the authentication with the data transfer unit which outputs the data demand hysteresis information containing said identifier of the data demand terminal unit [moreover,] Said said outputted data demand hysteresis information is acquired. By the predetermined criterion It is the management-criteria creation system equipped with the management equipment which judges whether the data demand terminal unit contained in the data demand hysteresis information is regular, is based on the judgment result, and creates or updates management criteria.

[0033]

[Embodiment of the Invention] Below, the gestalt of operation of this invention is explained with reference to a drawing.

[0034] (Gestalt of the 1st operation) Drawing 1 is the block diagram showing the management-criteria creation structure of a system in the gestalt of 1 operation of this invention, and it describes the management-criteria creation structure of a system of the gestalt of this operation, referring to this drawing below. In addition, with the gestalt of this operation, the same sign was fundamentally given to the thing of the same configuration, and the detailed explanation was abbreviated to what was explained by drawing 12 .

[0035] the [1st STB120 and ... to which management equipment 110 exists in every place as shown in drawing 1 , and] -- it is equipment which manages nSTB130 and each terminal unit. Moreover, management equipment 110 is a means to create and distribute the inaccurate equipment list of [for each STB to use in authentication]. The telephone line 140 is a means to use for the data transmission between management equipment 110 and each STB120,130. the gestalt of this operation -- 1st STB120 -- A Mr. ** of Hokkaido -- the [moreover,] -- nSTB presupposes that it is prepared in N Mr. ** of Okinawa.

[0036] Moreover, the terminal unit is connected to each STB120,130 on the data transmission line 1070, respectively. that is, VTR equipment 1030, VTR equipment 1040, a recording device 1050, and TV equipment 1060 connect with 1st STB120 as shown in this drawing -- having -- **** -- the [moreover,] -- VTR equipment 150, a recording device 160, and TV equipment 170 are connected to nSTB130. Here, suppose that VTR equipment 150 is inaccurate equipment. This inaccurate equipment shall be equipment manufactured by injustice as the license key mentioned later and EUI64 by copying the thing of the VTR equipment 1030 of normal as it is just as it is.

[0037] In addition, each [these] terminal unit is equipped with IEEE1394 as a data transfer means 1031 as drawing 12 explained it. Moreover, with the gestalt of this operation, these terminal units are beforehand equipped with EUI64 in IEEE1394 as the number of each equipment proper, i.e., an identification number, respectively. Here, EUI64 is 64-bit identification code. Moreover, these terminal units are equipped with the license key corresponding to the identification number. Although this license key is a secret private key given only to the terminal unit of normal, the identification number of EUI64 is the so-called ID number which anyone can know on the occasion of data transfer etc. Hereafter, the identification number of EUI64 is only called EUI64 or an ID number. In addition, EUI64 of a proper is prepared also about each STB120,130. To each equipment, these identification numbers support one to one, and do not overlap.

[0038] Next, the internal configuration of STB120 is further stated to a detail, referring to drawing 2 .

[0039] In addition to the configuration of the authentication means 1023 stated by drawing 12 , STB120 is equipped with the data demand hysteresis information storage means 212, a modem 213, the CRL record means 214, and the CRL storing means 215 as shown in drawing 2 .

[0040] The authentication means 211 are a point equipped with the service key generating function which can make the service key which is the same key as a license key, and the point which takes into consideration the list of the inaccurate equipment mentioned later in authentication, and are different from the authentication means 1023 stated by drawing 12 . This service key generation function is a function which generates a service key from EUI64 (ID number) obtained from the terminal unit. Therefore, the authentication means 211 does not need to memorize EUI64 of a terminal unit beforehand.

[0041] The data demand hysteresis information storage means 212 is a means to generate the hysteresis information about the data demand, and to memorize through the authentication mentioned later each time about what the transfer of requested data completed, when there is a data transfer demand of a predetermined program from a terminal unit. This data demand hysteresis information consists of EUI64 of the terminal unit which carried out the data transfer demand, time information which specifies time of day with the data demand from that terminal unit, and location information which specifies the location of that terminal unit. In addition, the data demand hysteresis information storage means 212 acquires these EUI(s) information - location information from the authentication means 211. Moreover, the data demand hysteresis information storage means 212 accumulates such hysteresis information from each terminal unit for one month, and is a means sent to management equipment 110 through a modem 213 for every month.

[0042] Moreover, the CRL record means 214 is a means which obtains the list data which indicated the inaccurate equipment sent from management equipment 110 from a modem 213, and is recorded and updated at the CRL storing means 215. The CRL storing means 215 is a memory means for storing the list data of inaccurate equipment. In addition, on these descriptions, the list of inaccurate equipment is only called CRL (Certification Revocation List). Moreover, the management criteria of this invention according to claim 1 correspond to CRL.

[0043] Next, the internal configuration of management equipment 110 is further stated to a detail, referring to drawing 3 .

[0044] The hysteresis information storage means 112 is a means to make each data demand hysteresis information transmitted to a coincidence term for every month from each STB120,130 correspond with EUI64 of STB of a transmitting agency, and to memorize it temporarily through a modem 111 as shown in drawing 3 . The inaccurate equipment decision means 113 is a means to determine the data demand terminal unit which has EUI64 which compares the time information and location information corresponding to EUI64 on these plurality, respectively, and has unjust possibility in all the data demand hysteresis information for 1 month from each STB memorized by the above-mentioned hysteresis information storage means 112 when two or more same EUI(s)64 exist. The CRL creation means 114 is a means to obtain the above-mentioned decision result outputted for every month from the inaccurate equipment decision means 113, to create the list of inaccurate equipment, and to output. All the CRL storage means 115 are means to obtain the list data from the CRL creation means 114, to make addition of new inaccurate equipment, correction of data, etc. to the already accumulated list, and to memorize all CRL(s) about the terminal unit of all areas. The individual CRL creation means 116 is a means to transmit to STB which creates CRL according to individual corresponding to each STB, and corresponds through a modem 111. CRL according to individual is the list of the inaccurate equipment packed for every STB, and is not created about STB by which inaccurate equipment is not detected.

[0045] Mainly referring to drawing 4 – drawing 6 (c), actuation of the gestalt of this operation is described and the gestalt of the 1 operation which relates to the management-criteria creation approach of this invention simultaneously is also explained [in / next / the above configuration]. In addition, drawing 4 is drawing explaining the content of storage of the data demand hysteresis information storage means 212 in STBs120 from January 1, 1997 to the 31st of the same month, and drawing 5 is drawing explaining the content of storage of the hysteresis information storage means 112 in the management equipments from January 1, 1997 to the 31st of the same month.

[0046] Here, as of January 31, 1997, inaccurate equipment is not yet indicated by CRL (list of inaccurate equipment) of the CRL storing means 215 of STB120, namely, presupposes at it that it is in an empty situation. Moreover, it is sky condition also about CRL of the CRL storing means of STB130.

[0047] Moreover, explanation here describes the authentication actuation using CRL in (1) STB first, next describes distribution of CRL to the creation of CRL and STB in (2) management equipment, and states the updating actuation of CRL in (3) STB to the last.

(1) Authentication actuation using CRL in STB : here, STB120 performs the following authentication actuation for the transfer request from the VTR equipment 1030 which

is equipment of normal a carrier beam case about AV data of the program which received with the receiving means 1021. In addition, this transfer request supports the demand which suited at 12:10 a.m. on January 10, Heisei 10 in the hysteresis information indicated in drawing 4 and drawing 5 .

[0048] Step 1: The authentication means 211 of STB120 obtains first EUI64 (here, they may be No. 11030) of the VTR equipment 1030 which has carried out the transfer request from the data transfer means 1024.

[0049] Step 2: and the authentication means 211 confirm whether the same number as the EUI64 is registered in CRL as a number of inaccurate equipment with reference to CRL of the CRL storing means 215. At this event, since CRL is sky condition as above-mentioned, a judgment result [having not registered] comes out and that EUI64 starts full-scale authentication (step 3). In addition, if a judgment that it registers with CRL comes out in this check phase, subsequent authentication will not be performed and a data transfer with a demand will not be performed, either.

[0050] Step 3: The authentication means 211 generates a service key from a service key generation function using EUI64 of the VTR equipment 1030 obtained at step 1. Thus, the generated service key is the same key as the license key which VTR equipment 1030 has. In addition, a license and a service key correspond to the secrecy function Sa stated by drawing 12 .

[0051] On the other hand, VTR equipment 1030 performs the same authentication as what was already explained by drawing 12 among both sides using the license key which it has beforehand using the service key which carried out the authentication means 211 in this way, and was generated. That is, both equipments generate the same subkey Ksa using random numbers A1 and B1, respectively.

[0052] Step 4: Using the above-mentioned subkey Ksa, the encryption means 1022 enciphers the work-piece key Kw, and enciphers AV data using the work-piece key Kw, and transmits the encryption data (Ksa (Kw), Kw (AV)) of these both sides to VTR equipment 1030.

[0053] Supposing EUI64 which is the process of this authentication, for example, has been sent from the terminal unit is the random number which does not have the response relation beforehand determined as the license key which that terminal unit has, it stops in addition, corresponding with that license key at all. [the key's generated by the service key generation function] because, a service key generation function -- the account of a top -- it is because it is constituted based on the response relation defined beforehand so that a service key may be generated from EUI64. Therefore, the data transfer which the above-mentioned authentication on condition of the key which both equipments have in this case being the same stops having materialized, and was demanded in this case is not performed.

[0054] Step 5: As EUI64 of the VTR equipment 1030 which is the destination, as No. 11030 and time information with a demand, the data demand hysteresis information storage means 212 acquires each information at 12:10 a.m. on January 10, Heisei 10, and records it as data demand hysteresis information from the authentication means 211 about what data transfer completed at step 4 (refer to drawing 4). Here, the publication of drawing 4 is explained. That is, in this drawing, No. 31060 as each number indicated by the column 401 of EUI64 of a terminal unit, No. 11040, No. 11030, and No. 21050 show EUI64 of TV equipment 1060, VTR equipment 1040, VTR equipment 1030, and a recording device 1050 sequentially from before.

[0055] Step 6: Whenever there is a data transfer demand from each terminal units 1030-1060, perform the above-mentioned steps 1-5 like the above. And the data demand hysteresis information storage means 212 makes what attached the telephone number as EUI64 (here, they may be No. 90001) and its location information on STB120 to each historical data (refer to drawing 4) by which record are recording was carried out in one month data demand hysteresis information (it transmits to management equipment 110 for every month through the telephone line 140 from a modem 213.).

(2) Creation of CRL in management equipment, and distribution actuation of CRL to STB : here, describe actuation of management equipment 110.

[0056] Step 101: The data demand hysteresis information mentioned above for every month is transmitted to the hysteresis information storage means 112 of management equipment 110 through a modem 111 from STBs 120-130 of every place. The hysteresis information storage means 112 holds such information as hysteresis information.

[0057] Step 102: The inaccurate equipment decision means 113 acquires the hysteresis information held at the hysteresis information storage means 112, and rearranges the content of data into time order by the time information (refer to drawing 5). Drawing 5 is drawing for explaining the content of the rearranged hysteresis information.

[0058] And if there is what has EUI64 [same] of the terminal unit shown in the column 501 (refer to drawing 5) of EUI64 of a terminal unit, the time information and location information corresponding to them will be compared, respectively, and the terminal unit corresponding to EUI64 with unjust possibility will be determined.

[0059] That is, when shown in drawing 5 , all EUI64 of the terminal unit indicated by each line to which the sign 511,512,513 was given is No. 11030. Then, these are checked first. When the time information of the line to which signs 511 and 512 were given is compared, it is the hysteresis of the transfer request in time of day different, respectively, and it can be judged that there is no conflict in both hysteresis. However, it is shown that the situation which is contradictory to the premise of not existing has generated the equipment which has EUI64 with two same hysteresis indicated by the line which attached signs 512 and 513. In addition, the number 90002 indicated by the column 504 of EUI64 of STB of drawing 5 is EUI64 of STB130.

[0060] Namely, when the inaccurate equipment decision means 113 compares the data of the column 502 of the time information of these both sides, and the column 503 of location information, it is a 10-minute [after the location where one side calls it Okinawa and another side is called Hokkaido and which was left distantly geographically] difference. It sees from the data that there was a transfer request with the equipment which has same EUI64, and the equipment which has same EUI64 judges that it exists in A Mr. ** of Hokkaido, and N Mr. ** of Okinawa. And the both sides of the equipment of these both sides consider that the inaccurate equipment decision means 113 is inaccurate equipment, and it sends the judgment result to the CRL creation means 114. In addition, till the place which says any are actually inaccurate equipment, although the VTR equipment 150 currently installed in N Mr. ** of Okinawa is actually inaccurate equipment, since it does not understand, in this phase, it considers that both sides are inaccurate for the time being. In addition, about the judgment with inaccurate any, it mentions later. Moreover, the situation which is contradictory to the premise that the equipment which has same EUI64 from the result of having compared the historical data indicated by the line which attached the sign 521,522 does not exist is not found.

[0061] Step 103: From the judgment result obtained from the inaccurate equipment decision means 113, the CRL creation means 114 creates CRL as shown in drawing 6 (a), and sends it to all the CRL storage means 115. Such creation actuation of CRL is performed every month, and it memorizes to whenever [the] at all the CRL storage means 115. Therefore, with the list sent from the CRL creation means 114, all the CRL storage means 115 add an addition, correction, etc. to already memorized CRL, and update them each time.

[0062] Step 104: The individual CRL creation means 116 looks at the column 601 of EUI64 of STB in CRL created with the CRL creation means 114, and separates the content of CRL for every STB. drawing 6 (b) and (c) were created, respectively in order to distribute to STB130 and STB120 -- individual -- it is CRL. The individual

CRL creation means 116 distributes these individual lists to corresponding STB through a modem 111.

(3) it has distributed from the updating actuation:management equipment 110 of CRL in STB -- individual -- STB120 which obtained CRL (refer to drawing 6 (c)) performs the following actuation.

[0063] step 201:214, i.e., a CRL record means, -- the above from a modem 213 -- individual -- CRL is obtained and it records on the CRL storing means 215 which was sky condition till then. Thereby, connection, now the VTR equipment 1030 (EUI64 is No. 11030) which is are registered into the CRL storing means 215 by STB120 as inaccurate equipment. Therefore, since it becomes clear that it is inaccurate equipment in the phase of the above-mentioned step 2 even if there will be a data transfer demand from this VTR equipment 1030 from now on, there is no data transfer limping gait ******. Thereby, amplification of the damage by inaccurate equipment can be prevented. In addition, also in STB130, same actuation is completely performed. In this case, VTR equipment 150 (EUI64 is No. 11030) is registered into the CRL storing means of STB130 as inaccurate equipment.

[0064] (Gestalt of the 2nd operation) Drawing 7 and 8 are the block diagrams showing the configuration of STB which constitutes the management-criteria creation system in the gestalt of 1 operation of this invention, and management equipment, and they describe the management-criteria creation structure of a system of the gestalt of this operation, referring to this drawing below. In addition, with the gestalt of this operation, the same sign was fundamentally given to the thing of the same configuration, and the detailed explanation was abbreviated to what was explained with the gestalt of the 1st operation. Moreover, the configuration of the whole system of the gestalt of this operation is the same as what was fundamentally stated by drawing 1 .

[0065] The main points of difference between the gestalt of this operation and the gestalt of the above-mentioned implementation are the processes of creation of the injustice and normal judging information about a terminal unit. Therefore, it explains focusing on this point of difference here. In addition, the management criteria of this invention according to claim 5 correspond to injustice and normal judging information.

[0066] In the configuration of STB120 shown in drawing 7 , the main points which are different from the configuration shown by drawing 2 are that the new contact detection means 711, injustice and a normal information storing means 712, and injustice and a normal information record means 713 are established instead of the data demand hysteresis information storage means 212 of drawing 2 , the CRL storing means 215, and the CRL record means 214. Furthermore, unlike what was stated with the gestalt of the 1st operation, the authentication means 714 does not have composition which outputs the hysteresis information about the data transfer demand from a terminal unit. In addition, other configurations are the same.

[0067] The new contact detection means 711 is a means to detect it and to acquire the EUI64, when there is equipment newly connected to the data transmission line 1070 of STB120. Acquired EUI64 attaches EUI64 of STB120, and is sent to management equipment 110 from a modem 213. This actuation is an activity for the new registration to the management equipment of the newly connected equipment, and is also an activity for checking simultaneously whether that new contact is inaccurate. In addition, since this actuation is performed in the case of new registration, unlike what is performed at every data transfer demand stated with the gestalt of implementation of the above 1st, it is first-time actuation.

[0068] Injustice and the normal information record means 713 are means to store in injustice and the normal information storing means 712 the information sent from management equipment 110.

[0069] Next, the configuration of management equipment 110 is described, referring to drawing 8 .

[0070] As shown in this drawing, the enquiry means 811 obtains EUI64 of STB of the EUI64 and transmission [of those] origin of the terminal unit which is sent from STBs 120-130 and which was newly established as new registration information, and is a means to judge whether it is inaccurate. The new registration equipment list information storage means 812 is a means to memorize EUI64 of the new registration equipment obtained from the enquiry means 811.

[0071] Moreover, injustice and the normal judging information creation means 813 are means to create the judgment information on whether to be inaccurate or regular about the equipment which had new registration from the above-mentioned check result by the enquiry means 811, and to transmit which the information to corresponding STB through a modem 111. In addition, when it becomes duplication registration, injustice and the normal judging information creation means 813 consider that the equipment of the both sides which have the EUI64 is inaccurate equipment, and creates and distributes the list (refer to drawing 6 (b) and (c)) of unjust information which corresponds for every STB.

[0072] Mainly referring to drawing 9 (a) - drawing 10 (b), actuation of the gestalt of this operation is described and the gestalt of the 1 operation which relates to the management-criteria creation approach of this invention simultaneously is also explained [in / next / the above configuration]. In addition, on account of explanation, the VTR equipment 1040 shown in drawing 1 , a recording device 1050, and TV equipment 1060 are connection settled at STB120, and they shall be connection settled at STB130, and, as for VTR equipment 150, a recording device 160, and TV equipment 170, the new registration as which it is explained at ** and the following shall also already be just managed with the gestalt of this operation to these terminal units. Moreover, VTR equipment 1030 presupposes that it is equipment newly connected to STB120. In addition, VTR equipment 150 presupposes that it is inaccurate equipment as the gestalt of the above-mentioned implementation also explained it. First, explanation here describes the detection actuation of the equipment connected newly in (1) STB, next describes the authentication actuation which used the renewal of injustice and normal judging information, and the injustice and the normal judging information in (3) STB at the last about creation of the new registration, and the injustice and the normal judging information in (2) management equipment etc. In addition, these explanation is given focusing on a point of difference with the gestalt of the 1st operation.

(1) Actuation in STB : suppose that VTR equipment 1030 was newly connected to STB120 as above-mentioned (refer to drawing 7).

[0073] Step 201: The new contact detection means 711 shown in drawing 7 reads periodically EUI64 of all the terminal units connected to the data transmission line 1070, and records it on the memory (graphic display abbreviation) to build in. And it compares with the newest record data of EUI64 of the terminal unit already recorded.

[0074] In the situation that VTR equipment 1030 was newly connected, the periodical thing of the above EUI64 it read and the equipment of No. 11030 was newly connected [the thing] for EUI64 by the above-mentioned comparison actuation is detectable.

[0075] Step 202: Transmit the new contact detection means 711 to management equipment 110 through a modem 213 further by making into new registration information EUI64 (No. 11030) of the equipment set as the object of the new registration which carried out [above-mentioned] detection, and EUI64 (No. 90120) of STB120 of a transmitting agency.

(2) Actuation in management equipment : drawing 9 (a) is drawing for explaining the content of storage of the new registration equipment list information storage means 812 before registering VTR equipment 1030, and drawing 9 (b) is drawing after VTR equipment 1030 was registered. It explains referring to these drawings.

[0076] Step 301: The enquiry means 811 shown in drawing 8 investigates the content of storage of the new registration equipment list information storage means 812 (refer to drawing 9 (a)) based on the new registration information transmitted from SBT120, and the registration confirms whether produce the situation of duplication registration. EUI64 contained in new registration information is No. 11030, and this overlaps a thing [finishing / registration / already] (the sign 901 was attached among drawing 9 (a)) as it shows drawing 9 (a). Therefore, about EUI64 of the duplicate both sides, the enquiry means 811 judges with it being inaccurate, and outputs.

[0077] Step 302: The new registration equipment list information storage means 812 registers the content of the new registration information sent from the enquiry means 811 (the sign 902 was attached among drawing). Furthermore, the information on an unjust purport is recorded on a remarks column 903 about EUI64 of the duplicate both sides from the above-mentioned judgment result. In addition, about the judgment with really inaccurate any, it mentions later.

[0078] Step 303: Injustice and the normal judging information creation means 813 create the list of injustice and normal judging information as shown in drawing 10 (a) and (b) from the judgment result sent from the enquiry means 811. These lists are packed for every STB. In drawing 10 (a) and (b), the information which shows injustice is recorded on the column 101 of a judgment result as above-mentioned. However, when judged with it being regular as a result of the judgment of the new registration information by the enquiry means 811 in step 301, the information which shows normal needless to say is recorded on the column 101 of a judgment result.

[0079] Step 304: Injustice and the normal judging information creation means 803 transmit the individual list of judgment results created as mentioned above to STB120 and STB130 through a modem 111. This transmission is performed whenever the new registration information mentioned above is sent from STB.

[0080] (3) Actuation in STB : drawing 11 (a) is drawing showing the content already stored in injustice and the normal information storing means 712, and shows the situation before transmitting the individual list of judgment results shown in drawing 10 (a). Moreover, drawing 11 (b) shows the situation after the content of the individual list of judgment results shown in drawing 10 (a) was reflected.

[0081] The injustice and the normal information record means 713 shown in drawing 7 obtain the individual list of judgment results transmitted from management equipment 110 from a modem 213, and adds it to the content of record shown in drawing 11 (a). The content of the above-mentioned individual list is added to the 4th line (the sign 1113 was attached among drawing) from on drawing 11 (b). The column 1111 of the judgment result of this drawing shows whether the equipment shown in the column 1112 of EUI64 of a registration terminal unit is inaccurate or regular.

[0082] On the other hand, also in STB130, the completely same actuation as the above is performed.

[0083] Next, the case where there is an AV data transfer demand is described from VTR equipment 1030 to STB120.

[0084] In this case, in the authentication actuation stated at step 1 stated with the gestalt of the 1st operation - step 4, since only the contents of the above-mentioned step 2 differ, only that point of difference is described.

[0085] That is, the authentication means 714 confirms whether EUI64 of the terminal unit which advanced the transfer request is regular or inaccurate with reference to injustice and the normal information storing means 712 after the same actuation as the above-mentioned step 1. According to the information recorded on the line which attached the sign 1113, it is shown that the equipment of No. 11030 has unjust EUI64 which has carried out the above-mentioned transfer request as shown in drawing 11 (b). Therefore, the authentication means 714 does not perform subsequent authentication and does not perform a data transfer with a demand, either.

[0086] In addition, as a result of a check, when regular, the same actuation as the content stated at the above-mentioned steps 3-4 is performed.

[0087] Moreover, in EUI64 of equipment with a transfer request not being registered into injustice and the normal information storing means 712, it is directed that the authentication means 714 sends the new registration information on the equipment of the demand origin to management equipment 110 to the new contact detection means 711. Thereby, amplification of the damage by inaccurate equipment can be prevented.

[0088] By the way, it is **** about the judgment with the any really inaccurate when it is judged with both equipments being inaccurate as mentioned above.

[0089] In this case, since the user who did not have data which it was considered by STB that it was inaccurate and were demanded transmitted tumefies the misgiving of carrier beam equipment for that unjust judging, he can request examination from the management pin center,large which owns management equipment 110. It confirms certainly whether be what the carrier beam management pin center,large investigated the truth of the equipment, and was manufactured or converted by the unjust approach in the examination request. And if it turns out to be regular, the data currently recorded on management equipment will be corrected and the correction result will be transmitted to corresponding STB. A transfer request will be accepted to the equipment which turned out to be regular by this.

[0090] Moreover, a magnetic-recording medium, an optical recording medium, etc. which recorded the program for making a computer perform any of the gestalt of the operation described above or all or a part of steps (means) of each steps (or means) of one publication can be created, and the same actuation as the above can also be performed using this. The same effectiveness as the above is demonstrated also in this case.

[0091] In addition, although the gestalt of the above-mentioned implementation described the case where it recorded on the data demand hysteresis information storage means 212 for all data transfer demands that existed from the terminal unit, the configuration recorded only for a data transfer demand not only this but important, for example may be used. Here, it is data like paper lek (PREC) or a paper view (PPV) of charging as important data, for example if it records. What follows, for example, pays money for every chain flannel, the program data of a free channel, etc. are good also as outside of an object.

[0092] Moreover, although the gestalt of implementation of the above 2nd described the case where it was detected automatically that the terminal unit was newly connected, the registration postcard is attached not only to this but to the equipment purchased newly, for example, and it is good also as a configuration whose user sends the postcard to the management pin center,large which owns management equipment.

[0093] Moreover, although the gestalt of the above-mentioned implementation described the case where transmission to STB of CRL, or injustice and normal information was performed using the telephone line, you may send not only by this but by broadcast.

[0094] Moreover, although the gestalt of implementation of the above 2nd described the case where compared the new registration information sent from the STB side with the already sent are recording data of new registration information, and it checked for no duplication It may have the memory holding the list data of EUI64 of normal equipment [finishing / production] indicated by the production information sent from each company which manufactured not only this but equipment, and the configuration of also performing the comparison with the content of the memory may be used in the case of the above-mentioned comparison. If it is the number which does not correspond even when EUI64 contained in new registration information is completely random, it is not recorded on the new registration equipment list information storage means 812 even if, but even if it is in the situation not overlapping, it can judge with it being inaccurate and the effectiveness of unjust prevention will improve more.

[0095] Moreover, the gestalt of the above-mentioned implementation is available even for even referring to not only this but only referring to CRL as for example, a content of authentication, or injustice and normal information, although the case where full-scale authentication actuation was performed was described.

[0096] Moreover, using a computer, processing actuation of each means of the gestalt of the above-mentioned implementation may be realized by software by work of a program, or may realize the above-mentioned processing actuation in hard by circuitry characteristic [without using a computer].

[0097] Moreover, although the data transfer unit of the invention in this application was STB with the gestalt of the above-mentioned implementation, and the case where the new registration information on the data demand equipment was transmitted to management equipment was explained when the STB detected connection with STB of the data demand terminal unit connected newly Not only in this, for example, the new contact detection means 711 If there is no same thing as compared with EUI64 of the terminal unit which obtains EUI64 of the VTR equipment 1030, already checks new connection, and is recorded when authentication is newly required from VTR equipment 1030 The configuration detected as what was connected newly is sufficient as the VTR equipment 1030.

[0098] Moreover, although the example of having sent the data demand hysteresis information which contains the identifier (EUI64) of the data demand terminal unit from a data transfer unit (STB) to management equipment was explained with the gestalt of the above-mentioned implementation when it was able to be checked as a result of authentication that it is regular equipment, the configuration of it not being concerned with the result of not only this but authentication, but sending the data demand hysteresis information to management equipment is used. In this case, what is necessary is just to send with hysteresis information also that, when it becomes clear that it is inaccurate equipment in process of authentication.

[0099] Moreover, although the gestalt of the above-mentioned implementation described the case where the management criteria (CRL, or injustice and normal judging information) of the invention in this application were used, in authentication actuation of STB, not only as this but an STB, the configuration which uses neither Above CRL, nor injustice and normal judging information may be used in the authentication actuation.

[0100]

[Effect of the Invention] This invention has the advantage in which detection of inaccurate equipment can be ensured compared with the former so that clearly from the place described above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the management-criteria creation structure of a system in the gestalt of 1 operation of this invention.

[Drawing 2] The block diagram showing the internal configuration of STB in the gestalt of this operation

[Drawing 3] The block diagram showing the internal configuration of the management equipment in the gestalt of this operation

[Drawing 4] Drawing explaining the content of storage of the data demand hysteresis information storage means of STB in the gestalt of this operation

[Drawing 5] Drawing explaining the content of storage of the hysteresis information storage means of the management equipment in the gestalt of this operation

[Drawing 6] (a): Drawing explaining CRL created by the CRL creation means in the gestalt of this operation

(b) -- it was created by the individual CRL creation means in the gestalt of the -(c):said operation -- individual -- drawing explaining CRL

[Drawing 7] The block diagram showing the internal configuration of STB in the gestalt of another operation

[Drawing 8] The block diagram showing the internal configuration of the management equipment in the gestalt of this operation

[Drawing 9] (a): Drawing for explaining the content of storage of a new registration equipment list information storage means before registering the VTR equipment in the gestalt of this operation (b): Drawing for explaining the content of storage of a new registration equipment list information storage means after the VTR equipment in the gestalt of this operation was registered

[Drawing 10] (a) Drawing explaining the individual list of the injustice and normal judging information created by -(b):injustice and the normal judging information creation means

[Drawing 11] (a): Drawing showing the content of storing in injustice and a normal information storing means before transmitting the individual list of judgment results shown in drawing 10 (a)

(b): Drawing showing the content of storing in injustice and a normal information storing means after the individual list of judgment results shown in drawing 10 (a) was transmitted

[Drawing 12] The block diagram showing the conventional connection situation and conventional configuration of an exclusive receiver and a terminal unit

[Description of Notations]

110 [ ] Management Equipment
120 [ ] 1st STB
130 [ ] the -- NSTB
150, 1030, 1040 VTR equipment
160 1050 Recording device
170 1060 TV equipment
1010 Antenna